

OCT 03 2007

Applicant: Mike C. Robinson et al.

Serial No.: 10/061,619

Filed: February 1, 2002

Docket No.: 100200201-1

Title: SECURE INITIALIZATION OF COMMUNICATION WITH A NETWORK RESOURCE**IN THE CLAIMS**

Please amend claims 1, 5, 13, 17, 19, 26, 30, 36, 40, 41, 45, 47, and 51 as follows:

1. (Currently Amended) A method for initialization of secure communication between a network resource and a client via a network, comprising:

receiving ~~unsecured access~~ access in an unsecured mode to the network resource from a management application of the client via the network;

~~in response to the unsecured access~~ in the unsecured mode, generating configuration parameters for initializing secure communication between the network resource and the client via the network;

printing a security configuration page showing the configuration parameters for initializing secure communication between the network resource and the client;

receiving manual input of the configuration parameters into the management application of the client; and

after receiving manual input of the configuration parameters, implementing secure communication between the network resource and the management application of the client in accordance with the configuration parameters.

2. (Previously Presented) The method of claim 1 wherein the network resource is a print server and the security configuration page is printed using a printer coupled to the print server.

3. (Original) The method of claim 1 wherein the secure communication is in accordance with a version of SNMPv3 standards.

4. (Previously Presented) The method of claim 1 further comprising:  
generating random security parameters to generate the configuration parameters for initializing the secure communication.

OCT 03 2007

Applicant: Mike C. Robinson et al.

Serial No.: 10/061,619

Filed: February 1, 2002

Docket No.: 100200201-1

Title: SECURE INITIALIZATION OF COMMUNICATION WITH A NETWORK RESOURCE

5. (Currently Amended) The method of claim 1 further comprising:  
setting a security configuration print page object in response to receiving the ~~unsecured access contact~~ from the management application.
6. (Original) The method of claim 5 wherein the security configuration print page object is in accordance with a version of SNMPv3 standards.
- 7-12. (Cancelled)
13. (Currently Amended) A system for initialization of secure communication between a network resource and a client via a network, comprising:  
means for receiving ~~unsecured access~~ access in an unsecured mode to the network resource from a management application of the client via the network;  
means for generating configuration parameters for initializing secure communication between the network resource and the client via the network, ~~in response to the unsecured access~~ while in the unsecured mode;  
means for printing a security configuration page showing the configuration parameters for initializing secure communication between the network resource and the client;  
means for receiving manual input of the configuration parameters into the management application of the client; and  
means for implementing secure communication between the network resource and the management application of the client in accordance with the configuration parameters after receiving manual input of the configuration parameters.
14. (Original) The system of claim 13 wherein the network resource is a print server and the security configuration page is printed using a printer coupled to the print server.
15. (Original) The system of claim 13 wherein the means for implementing secure communication are in accordance with a version of SNMPv3 standards.

Applicant: Mike C. Robinson et al.

Serial No.: 10/061,619

Filed: February 1, 2002

Docket No.: 100200201-1

Title: SECURE INITIALIZATION OF COMMUNICATION WITH A NETWORK RESOURCE

16. (Previously Presented) The system of claim 13 further comprising:  
means for generating random security parameters to generate the configuration parameters for initializing the secure communication.
17. (Currently Amended) The system of claim 13 further comprising:  
means for setting a security configuration print page object in response to ~~receiving~~  
~~the unsecured access contact~~ from the management application.
18. (Original) The system of claim 17 wherein the means for setting a security configuration print page object are in accordance with a version of SNMPv3 standards.
19. (Currently Amended) A network resource system for initializing secure communication with a client via a network, comprising:  
a network interface configured to receive ~~unsecured access~~ access in an unsecured mode via the network from a management application of the client; and  
an SNMP daemon configured to generate configuration parameters for initializing secure communication with the client via the network, ~~in response to the unsecured access~~  
while in the unsecured mode;  
wherein the SNMP daemon is configured to generate a configuration page event causing a printer coupled to the network resource to print a security configuration page showing the configuration parameters, and  
wherein upon manual input of the configuration parameters from the security configuration page into the management application of the client, secure communication with the client is implemented.
20. (Original) The system of claim 19 further comprising:  
an SNMP user table within a data structure of the network resource, the SNMP user table for access by the SNMP daemon and configured to store a user account created in accordance with the configuration parameters.
21. (Original) The system of claim 19 wherein the network resource is a print server.

Applicant: Mike C. Robinson et al.

Serial No.: 10/061,619

Filed: February 1, 2002

Docket No.: 100200201-1

Title: SECURE INITIALIZATION OF COMMUNICATION WITH A NETWORK RESOURCE

---

22. (Original) The system of claim 19 wherein the SNMP daemon is configured to implement secure communication in accordance with a version of SNMPv3 standards.
23. (Original) The system of claim 19 wherein the SNMP daemon is configured to generate random security parameters in order to generate the configuration parameters for initializing the secure communication.
24. (Original) The system of claim 19 wherein the network interface includes a plurality of interface components for interfacing with a corresponding plurality of network communication protocols.
25. (Previously Presented) The system of claim 24 wherein the network communication protocols include TCP/IP, IPX, and Apple Talk.
26. (Currently Amended) A method for initialization of secure communication between a network resource and a client via a network wireless access point, comprising:
- receiving ~~unsecured ad hoc access~~ ad hoc access in an unsecured mode to the network resource from a management application of the client;
  - ~~in response to the unsecured ad hoc access in the unsecured mode~~, generating a security key for initializing secure communication between the network resource and the client via a wireless access point;
  - printing a security configuration page showing the security key;
  - receiving manual input of the security key into the management application of the client;
  - receiving encrypted ad hoc access to the network resource from the management application in accordance with the security key for configuration of infrastructure mode parameters for the wireless access point; and
  - upon manual input of the security key from the security configuration page, implementing secure communication between the network resource and the management

Applicant: Mike C. Robinson et al.

Serial No.: 10/061,619

Filed: February 1, 2002

Docket No.: 100200201-1

Title: SECURE INITIALIZATION OF COMMUNICATION WITH A NETWORK RESOURCE

---

application of the client in accordance with the security key via the wireless access point in an infrastructure mode.

27. (Original) The method of claim 26 wherein the network resource is a print server and the security configuration page is printed using a printer coupled to the print server.

28. (Original) The method of claim 26 wherein the secure communication is in accordance with a version of 802.11 standards.

29. (Previously Presented) The method of claim 26 wherein the security key is a randomly generated 802.11 Wired Equivalent Privacy key for initializing the secure communication.

30. (Currently Amended) The method of claim 26 further comprising:  
setting a 802.11 security configuration print page object in response to receiving the ~~unsecured ad hoc access~~ contact from the management application.

31-35. (Cancelled)

36. (Currently Amended) A system for initialization of secure communication between a network resource and a client via a network wireless access point, comprising:

means for receiving ~~unsecured ad hoc access~~ ad hoc access in an unsecured mode to the network resource from a management application of the client;

means for generating a security key for initializing secure communication between the network resource and the client via a wireless access point ~~in response to the unsecured ad hoc access~~ while in the unsecured mode;

means for printing a security configuration page showing the security key;

means for receiving manual input of the security key into the management application of the client;

Applicant: Mike C. Robinson et al.

Serial No.: 10/061,619

Filed: February 1, 2002

Docket No.: 100200201-1

Title: SECURE INITIALIZATION OF COMMUNICATION WITH A NETWORK RESOURCE

---

means for receiving an encrypted ad hoc access to the network resource from the management application in accordance with the security key for configuration of infrastructure mode parameters for the wireless access point; and

means for implementing secure communication between the network resource and the management application of the client in accordance with the security key via the wireless access point in an infrastructure mode after receiving manual input of the security key.

37. (Original) The system of claim 36 wherein the network resource is a print server and the means for printing a security configuration page comprises a printer coupled to the print server.

38. (Original) The system of claim 36 wherein the means for implementing secure communication is in accordance with a version of 802.11 standards.

39. (Previously Presented) The system of claim 36 wherein the security key is a randomly generated 802.11 Wired Equivalent Privacy key for initializing the secure communication.

40. (Currently Amended) The system of claim 36 further comprising:  
setting a 802.11 security configuration print page object in response to receiving the ~~unsecured ad hoc access contact~~ from the management application.

41. (Currently Amended) A computer readable media having computer readable code which when executed by a computer system of a network resource causes the network resource to implement a method for initialization of secure communication between the network resource and a client via a network, comprising:

receiving ~~unsecured access~~ access in an unsecured mode to the network resource from a management application of the client via the network;

~~in response to the unsecured access in the unsecured mode,~~ generating configuration parameters for initializing secure communication between the network resource and the client via the network;

Applicant: Mike C. Robinson et al.

Serial No.: 10/061,619

Filed: February 1, 2002

Docket No.: 100200201-1

Title: SECURE INITIALIZATION OF COMMUNICATION WITH A NETWORK RESOURCE

---

printing a security configuration page showing the configuration parameters for initializing secure communication between the network resource and the client;

receiving manual input of the configuration parameters into the management application of the client; and

after receiving manual input of the configuration parameters, implementing secure communication between the network resource and the management application of the client in accordance with the configuration parameters.

42. (Original) The computer readable media of claim 41 wherein the network resource is a print server and the security configuration page is printed using a printer coupled to the print server.

43. (Original) The computer readable media of claim 41 wherein the secure communication is in accordance with a version of SNMPv3 standards.

44. (Previously Presented) The computer readable media of claim 41 further comprising: generating random security parameters to generate the configuration parameters for initializing the secure communication.

45. (Currently Amended) The computer readable media of claim 41 further comprising: setting a security configuration print page object in response to receiving the ~~unsecured access contact~~ from the management application.

46. (Original) The computer readable media of claim 45 wherein the security configuration print page object is in accordance with a version of SNMPv3 standards.

47. (Currently Amended) A computer readable media having computer readable code which when executed by a computer system of a network resource causes the network resource to implement a method for initialization of secure communication between the network resource and a client via a network wireless access point, comprising:

Applicant: Mike C. Robinson et al.

Serial No.: 10/061,619

Filed: February 1, 2002

Docket No.: 100200201-1

Title: SECURE INITIALIZATION OF COMMUNICATION WITH A NETWORK RESOURCE

receiving ~~unsecured ad hoc access~~ ad hoc access in an unsecured mode to the network resource from a management application of the client;

~~in response to the unsecured ad hoc access~~ in the unsecured mode, generating a security key for initializing secure communication between the network resource and the client via a wireless access point;

printing a security configuration page showing the security key;

receiving manual input of the security key into the management application of the client;

receiving encrypted ad hoc access to the network resource from the management application in accordance with the security key for configuration of infrastructure mode parameters for the wireless access point; and

upon manual input of the security key from the security configuration page, implementing secure communication between the network resource and the management application of the client in accordance with the security key via the wireless access point in an infrastructure mode.

48. (Original) The method of claim 47 wherein the network resource is a print server and the security configuration page is printed using a printer coupled to the print server.

49. (Original) The method of claim 47 wherein the secure communication is in accordance with a version of 802.11 standards.

50. (Previously Presented) The method of claim 47 wherein the security key is a randomly generated 802.11 Wired Equivalent Privacy key for initializing the secure communication.

51. (Currently Amended) The method of claim 47 further comprising:  
setting a 802.11 security configuration print page object in response to ~~receiving the unsecured ad hoc access contact~~ from the management application.